Amendments to the Specification:

Please replace the paragraph beginning on page 1, line 5, with the following rewritten paragraph:

-- This application claims priority to the following provisional patent applications, which ~~are~~ is incorporated herein by reference in ~~their~~ its ~~entireties~~entirety:--

Please replace the paragraph beginning on page 3, line 12, with the following rewritten paragraph:

-- The ANX VPN permits the use of a plurality of different IPSec devices. By virtue of the TEL-2 specification and the certification process all of the designated IPSec devices are guaranteed to communicate with one another across the ANX VPN.--

Please replace the paragraph beginning on page 3, line 24, with the following rewritten paragraph:

-- For example, when two companies want to communicate over the Internet, the lag between the systems at each company will be different virtually every time. The connection each has through ~~their~~ its service provider, i.e. 14.4K, 28.8K, 56K, ISDN, DSL, T1, etc., plus the number of servers through which the connection is directed contribute to the resulting time lag between the two companies. Depending upon the type of information transmitted, the two parties may require a maximum acceptable time lag. Due to the nature of the Internet, it cannot guarantee such a maximum time lag. Furthermore, the two companies may desire that service assistance be available at certain times or 24 hours a day. The Internet has no such guarantees for help availability in a multi-provider environment. Such a lack of guaranteed bandwidth, latency and reliability are major impediments to business-to-business commerce and communication over the Internet.--

Please replace the paragraph beginning on page 4, line 26, with the following rewritten paragraph:

-- The system and method of the present invention utilizes an overseer that defines the service quality, continually qualifies service providers as meeting that service quality, and resolves end-to-end issues across multiple interconnected virtual private networks, such as the ANX. When connecting multiple virtual private networks according to the system and method of the present invention multiple interconnect providers are interconnected, and the manner in which these interconnect providers are interconnected so that the quality and reliability standards ~~is~~ are met ~~are~~ is another aspect of the present invention.--

Please replace the paragraph beginning on page 6, line 28, with the following rewritten paragraph:

-- **Fig. 13** is a diagram illustrating a multiple virtual private network fee model for interconnection of two virtual private networks according to the present invention; ~~is a diagram illustrating interconnection of two virtual private networks using a multiple transit certified service providers according to the present invention;~~--

Please replace the paragraphs beginning on page 8, line 3, with the following rewritten paragraphs:

-- Fig. 1 shows a block diagram of two interconnected virtual private networks (VPN) 20 and 22. The present system and method of the interconnecting multiple virtual private networks is not intended to be limited to only these types of networks and has applicability to a wide variety of virtual private networks.

Each virtual private network 20 and 22 is shown having a trading partner (TP) 24 and 26, respectively. While Fig. 1 shows only one TP 24 and 26 for each virtual private network, there can in fact be hundreds or thousands of such TPs for each virtual private network. Fig. 1 is intended to define the end-to-end service quality concept, and for such a purpose, only one TP 24 and 26 is needed for each virtual private network 20 and 22.--

Please replace the paragraphs beginning on page 9, line 3, with the following rewritten paragraphs:

-- One resolution is shown in Fig. 3, in which each VPN 20 and 22 maintain their own governance, but the program management, coopetition policy, contracts, service assurance, and service description for the two VPNs 20 and 22 are unified. Such unification means that where the parameters for the program management, coopetition policy, contracts, service assurance, and service description of the two VPNs 20 and 22 are different, the parameter used in one of the networks is chosen as the acceptable minimum standard or a compromise parameter different from the parameter used in each ~~or~~ of the VPNs is agreed upon. It is possible that the parameters for communication within each VPN need not change, while the new parameters are used only when communicating between VPNs. Fig. 3 further shows that the system and method contemplate connecting more than two VPNs.

One configuration for governance of multiple interconnected VPNs is shown in Fig. 4. In this scenario each VPN has its own program overseer (POVER) 30, and a global, or multiple virtual private network, overseer (GOVER) 32 is provided to resolve issues between the POVERs 30. Arrows are shown between the POVERs 30 indicating that the POVERs 30 are free to resolve their issues without requiring the GOVER 32. The GOVER is called on when direct POVER-to-POVER resolution fails. Each of the POVERs 30 governs one of the regional VPNs, while the GOVER 32 oversees the interconnection of the VPNs.--

Please replace the paragraph beginning on page 10, line 4, with the following rewritten paragraph:

-- In the ANX type VPN each TP, CSP and CEP must meet specified criteria to become certified and to maintain that certification. The certification provides the TPs or subscribers with confidence that the level ~~or~~ of transport and security will meet their business needs. The ANX type VPN utilizes multiple CSPs. On one level it is easier to run a VPN where all TPs are required to use a single CSP. The use of multiple CSPs in the ANX type VPN fosters competition between the CSPs and allows the VPN to reach TPs that may not be serviced by a single CSP. The implementation of multiple CSPs, however, brings with it the drawback of

insuring that the CSPs can talk to one another. Whether the connection from one TP to another TP within the same VPN is through a single CSP of two CSPs should be invisible to the TPs. The TPs need never know when one or more CSPs are used for any particular connection. The certification process ensures that the TPs use one of the certified IPSec devices at their premises, and that the CSPs will utilize certified equipment and meet certain metrics so as to achieve the end-to-end service quality guaranteed to the TPs. In this manner, the multiple CSPs will be able to communicate with one another. The CSPs must meet business criteria, technical metrics, ongoing monitoring, trouble-handling criteria, routing registry criteria, and domain name registry criteria to achieve and maintain certification.--

Please replace the paragraphs beginning on page 11, line 4, with the following rewritten paragraphs:

-- Fig. 7 illustrates the end-to-end availability metric. The Access network, between the TP1 router 60 and the ANX CSP_1 62 is permitted to be unavailable 43.80 hours/year. The ANX CSP_1 62 may only be unavailable 2.63 hrs./year. The trunk 65 between the ANX CSP_1 62 and the ANX CEPO 64 may only be unavailable 1.76 hrs./year. The ANX CEPO 64 may only be unavailable 0.44 hours/year. The foregoing availabilities yield a total of 99.895% availability or 9.22 hours per year downtime.

The outline for how trouble is handled within the ANX-type VPN is shown in Fig. 8. There are effectively five layers of trouble handling. At the first level trouble between TPs is handled directly between the two TPs. Similarly, issues between the TPs and the CSPs are handled between the two parties. CSPs and the CEPOs also resolve their troubles between the troubled parties. A network overseer is provided to handle troubles that cannot be handled in the foregoing scenarios. The overseer can take complaints from the ~~TPS~~TPs, the CSPs, and the CEPOs.--

Please replace the paragraph beginning on page 12, line 4, with the following rewritten paragraph:

-- The GOVER/POVER model is but one way to oversee ensuring of the end-to-end service quality and metric compatibility. How the ANX-type networks are connected will be discussed below. In this context there must be five key types of end-to-end technology compatibility: 1 network interconnection that ensures a trading partner on one VPN can reach any trading partner on the other VPN; 2 routing compatibility that ensures any trading partner on one VPN can logically reach ~~nay~~ any TP on the other VPN; 3 naming compatibility, e.g. so the web names or e-mail names of any trading partner on one VPN can be resolved to an address that is routable over the two VPNs; 4 IPSec compatibility; and 5 digital security certificate compatibility across multiple VPNs. While Figs. 9 and 10 refer to regional/national VPNs and international arbitration, the VPNs need not be limited to a specific country or geographical area. Any ANX-type VPN, regardless of the location of its subscribers could be interconnected.--

Please replace the paragraph beginning on page 12, line 23, with the following rewritten paragraph:

-- Returning to the GOVER/POVER model for overseeing interconnected VPNs; Fig. 12 illustrates an end-to-end trouble escalation model. It is expected that CSPs will work together to resolve trouble before contacting a POVER. Similarly, the POVERs and/or the ~~POVERS~~ POVERs and the interconnect provider are expected to work together to resolve trouble before contacting the GOVER.--

Please replace the paragraph beginning on page 13, line 5, with the following rewritten paragraph:

-- There are multiple methods of interconnecting multiple VPNs with interconnect providers. As shown in Fig. 14, all the VPNs, having multiple service providers, can be interconnected using a single interconnect provider. Alternatively, all the VPNs can be interconnected by multiple interconnect providers, as shown in Fig. 15, thereby creating competition between the interconnect providers, just as there is competition between the CSPs in

a single xNX-type VPN. Finally, as shown in Fig. 16, where no suitable interconnect provider is available to connect all ~~he~~ the VPNs having multiple service providers, multiple interconnect providers are used. These interconnect providers service different combinations of VPNs. In Fig. 16, interconnect provider 120 interconnects VPNs having multiple service providers 122, 124, and 126. Interconnect provider 130 interconnects VPNs having multiple service providers 132 and 126. As a result, a TP of VPN 132 must connect through both Interconnect provider 130 and Interconnect provider 120 to reach TPs of either VPN 122 or 124.--

Please replace the paragraphs beginning on page 13, line 26, with the following rewritten paragraphs:

-- In Fig. 17b TP 200, CSP 210, exchange point 220 and Interconnect provider 300 are connected in the same manner shown in Fig. 17a. While the second TP 250 is connected to the CSP 260, the exchange point 270 is not provided. Instead CSP 260 is shown as connecting directly to the Interconnect provider 300. This embodiment encompasses the situation where the Interconnect provider 300 and CSP 260 are the same entity or are directly wired. Fig. 17c is similar to Fig. ~~16b~~17b,

~~Except~~ except that the ~~interconnect~~ Interconnect provider 300 also acts as a CSP 320, and a third TP 310 is connected directly to the Interconnect provider 300/CSP 320.

As stated previously, while the end-to-end service quality is based upon the TEL-2 specification, the degree to which the TEL-2 specification needs to be modified to interconnect multiple VPNs depends upon the chosen complexity of the interconnection. An xNX-type VPN uses a maximum of two CSPs between any two TPS. A larger value, either three or four, is needed for multiple VPNs. The Interconnect provider will account for one additional CSP, and for configuration set forth in Fig. 16, two Interconnect providers are employed in addition to the two CSPs yielding four CSPs.--